Pritchin I. R.
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Aleksandra Georgievna

INFORMATION TECHNOLOGY INFRASTRUCTURE SECURITY IN CYBERATTACKS

Abstract. *The planet has been encompassed by computerization; a huge, ever-increasing amount of information continuously runs on the World Wide Web. However, along with the rapid development of information technology, cyberattacks have evolved and become more sophisticated. The majority of recent most important cyber incidents, unlike basic disorganized threats, have been coordinated or specific attacks, called Advanced Persistent Threats. This paper presents phases and common mechanisms of these attacks.*

Keywords: *information security, cyber-incidents, sophisticated attacks, advanced persistent threats, Ural Federal University.*

Притчин И. Р.
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ ИНФРАСТУРКТУР ПРИ КИБЕРАТАКАХ

Аннотация. *Планету охватила компьютеризация, по всемирной паутине непрерывно курсирует огромное, постоянно возрастающее, количество информации. Однако, вместе с быстрым развитием информационных технологий, развивались и усложнялись кибератаки. В последние годы все больше инцидентов информационной безопасности являются хорошо спланированными и координированными атаками или «целевыми кибератаками». В статье рассматриваются стадии и основные механизмы таких атак.*

Ключевые слова: *информационная безопасность, компьютерные инциденты, развитые устойчивые угрозы, целевые кибератаки, Уральский Федеральный Университет.*

In recent years information technology and so-called cyberspace have been expanded significantly and evolved into a large, dynamic and tangled web of computing devices. There always have been cyber-attacks along with this rapid development. They have existed since the adoption of the Internet and have evolved a lot in the past decades, from viruses and worms in the early days to comprehensive malware and botnets nowadays. After a few recent sporadic large-scale security breaches it has become clear that attacks in cyber-space are not limited to government activities for intelligence purposes, but any part of critical and enterprise infrastructure may be a subject of attacks, from the banking system and utilities to the transport or supply of essential goods and commodities. As highlighted in such incidents, a new class of threats has emerged, the «Advanced Persistent Threat» (APT). Originally used to describe cyber-intrusions against military organizations, the APT has evolved and is no longer limited to the military domain.

The modes of APT are diverse, these attacks last for months, and they are hard to notice. Despite APT has drawn increasing attention from the industrial security community, a comprehensive and clear understanding of the APT research problem is lacking. Therefore, cyber-defense has become one of the most important issues in

national, production and enterprise defense strategies. This study presents an overview of the APT phenomenon, its taxonomy, stages and countermeasures.

APT is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception) 0. These objectives include intellectual property theft, compromising sensitive information, sabotaging of critical organizational infrastructures (databases, manufacturing pipelines). This kind of exfiltration of information often continues with blackmailing a company for profit 0. Common targets of APT attacks are industries, military, finance and banking, education, energy, healthcare, telecommunications operators, IT businesses 0. Since APT is an advanced type of attacks, it consists of many stages and concrete strategies, it pursues its objectives repeatedly over an extended period of time, it adapts to any types of defenses.

APT attacks differ from traditional threats in the following issues:

1) clear goal, efforts concentrated on specific target;
2) high-skilled and well-resourced coordinated attackers;
3) long-term campaign with repeated attempts, manual execution;
4) the perpetrator remains stealthy and uses evasive attack technics.

APT attacks are scrupulously planned, and often have several stages involved. Every APT attack has its own unique features (instruments and techniques), but the stages are similar. To describe the phases of an APT attack and to understand threat actors' techniques, the six-stage model based on the concept of an «intrusion kill chain» is demonstrated in the study.

A typical APT attack has the following six phases:

1) Reconnaissance and weaponization;
2) Delivery;
3) Initial intrusion;
4) Command and control, maintaining access;
5) Lateral movement;

6) Data exfiltration and covering up tracks.

In the step of reconnaissance and weaponization, attackers gather as much information about technical environment and personnel in targeted organization as possible. Attackers may use passive and active reconnaissance. Passive reconnaissance is an attempt to gain information about targeted organization's network without actively engaging with the systems. Possible techniques include eavesdropping and wardriving on public networks of targeted organization, using specialized search-engines, searching for e-mails, credentials, used software, leaked databases related to targeted organization in open sources. Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. Possible techniques include port scanning, OS fingerprinting, password spraying, brute-forcing directories and files names on web/application servers. The adversary may try to gather information from employees via social engineering techniques. During the substage of weaponization, attackers craft specific tools and exploits based on the results of reconnaissance and chosen approaches.

The phase of delivery refers to the delivery of the exploit crafted in the previous phase. There are two types of delivery mechanisms: direct and indirect. For direct delivery, attackers send exploits to their targets via various social engineering techniques, such as spear fishing. Or if there was severe vulnerability in the target's network perimeter, the attacker may directly break into vulnerable service or server. Indirect delivery is stealthy. In this approach the attackers will compromise a 3rd party that is trusted by the target, and then use the compromised 3rd party to indirectly serve exploits.

Initial intrusion happens when the attacker gets the first unauthorized access to the target's computer/network. Typical way for intrusion is executing malicious code that exploits vulnerability in the target's computer; however, the attackers may obtain access credentials through social engineering. As a result of this stage, the attackers establish a foothold in the target's network with persistent presence.

Lateral movement phase describes the steps taken once the communication between the compromised systems and C&C servers is established. The adversaries move inside the network, in order to expand their control and collect valuable data. This stage typically lasts a long period, because the attackers want to harvest a maximum of information and they want to remain unnoticed.

Data exfiltration is the most critical part of most APT attacks, because the primary goal of the attackers is to steal sensitive data. In order to avoid detection or alerts APT actors often use various stealthy tactics. Common methods of data exfiltration take advantage of «always available» types of network traffic, like DNS or NTP. By «stuffing» data into the headers of traffic types that are always able to leave a network, attackers retrieve data assets slowly over allowed protocols to avoid detection. Additionally, the data may be compressed and encrypted. APT actors often use secure protocols like SSL/TLS, or leverage the anonymity feature of Tor network to hide the transmission to external locations.

Final part, covering tracks, involves modifying any possible evidence like logs, files, registry from all applications and devices, which were somehow touched by an attack in the previous stages. This type of anti-forensic is crucial for the attackers, because otherwise they could be tracked down by incident response team.

APTs are sophisticated, specific and evolving threats, yet certain patterns can be identified in their process. The analyses of APT mechanisms and methods make the bases for further research of APT to define possible defense strategies.

REFERENCES

1. Ping C, Lieven D, Christophe H. A study on Advanced Persistent Threats. – 2014. – Text: electronic. – URL: https://link.springer.com/content/pdf/10.1007%2F978-3-662-44885-4_5.pdf (Reference date 27.12.2020). p. 64.

2. Ana K. Dragana N. Cyber Attacks on Critical Infrastructure: Review and Challenges (draft). – 2015. – Text: electronic. – URL: https://www.researchgate.net/profile/Ana_Kovacevic/publication/271515016_Cyber_Attacks_on_Critical_Infrastructure_Review_and_Challenges_draft/links/54ca54540cf2517b755df827/Cyber-Attacks-on-Critical-Infrastructure-Review-and-Challenges-draft.pdf (Reference date 27.12.2020). p. 8.

3. Do Xuan Cho, Ha Hai Nam. A Method of Monitoring and Detecting APT Attacks Based on Unknown Domains. – 2019. – URL: https://www.sciencedirect.com/science/article/pii/S1877050919304041/pdf?md5=0073c63fe2a4bf96c7e0c77a3491cc91&pid=1-s2.0-S1877050919304041-main.pdf (Reference date 27.12.2020). p. 317.